Inligtingsoorlogvoering, die opkomende magprojekteringinstrument: soeke na ’n definisie

Rianne van Vuuren
Universiteit van Stellenbosch

Abstract

Information warfare, an upcoming power projection instrument: in search of a definition

Information warfare has become an integral part of practically all international conflict situations. The most prominent recent manifestations include the Hamas-Israel conflict, the Estonia–Russia cyberwar and the Georgia-Russia war. While elements of this form of conflict are as old as humankind, the information age has created unique and new opportunities for information warfare to manifest as an upcoming national security threat in the 21st century. Despite the diverse, and sometimes even contradictory, definitions, the information revolution and growing global integration have ensured that information warfare is destined to become one of the most significant national security challenges in the future. After a critical presentation of broad, military and information technology-oriented definitions, information warfare is defined as actions focused on destabilising or manipulating the core information networks of a state or entity in society with the aim of influencing the ability and will to project power as well as efforts to counter similar attacks by an opposing entity and/or state. The core of this argument is that information as a power instrument can be used in both offensive and defensive roles. The definition proposed for information warfare encompass three forms of manifestation of information warfare, namely netwar, psychological operations and cyberwarfare. The differentiation between the three manifestations is done on a cognitive/technology continuum. This definition of information warfare provides an opportunity to identify the common elements and significant characteristics of this phenomenon. The foundations highlight the significance of networked relationships, the information revolution and digital age all central to the development of information warfare. At the same time modern conflict and war are manifesting within the context of the information age, ensuring that information warfare is becoming a significant national security threat. A thorough analysis of the manifestation and implications of information warfare in current and future conflicts in Africa, but also worldwide, would be necessary to understand conflict in its modern and future context.

ISSN 1995-5928 | Tel: 021 886 5169 | E-pos: akademies@litnet.co.za

Opsomming

Inligtingsoorlogvoering, die opkomende magprojekteringinstrument: soeke na 'n definisie

Inligtingsoorlogvoering het 'n integrale deel van bykans alle internasionale konfliksituasies geword, met die mees prominente onlangse voorbeelde die Hamas-Israel-konflik, die Estland–Rusland-kuberoorlog en die Georgië-Rusland-oorlog. Terwyl elemente van hierdie vorm van konflik so oud soos die mensdom en oorlog is, het die inligtingseeu unieke en nuwe geleenthede geskep vir inligtingsoorlogvoering om te manifesteer as 'n opkomende nasionale veiligheidsbedreiging in die 21ste eeu. Ten spyte van diverse, en somtyds teenstrydige, definisies wat aan die konsep verleen word, het die inligtingsrevolusie en groeiende globale integrasie verseker dat dit een van die mees betekenisvolle nasionale veiligheidsbedreigings van ons tyd sowel as van die toekoms word. Na 'n kritiese uiteensetting van breë, militêre en inligtingstegnologie-georiënteerde definisies word inligtingsoorlogvoering gedefinieer as aksies gefokus op die destabilisering of manipulasie van sentrale inligtingsnetwerke van 'n staat of entiteit in 'n gemeenskap met die doel om die vermoë en wil om mag te projekteer, te beïnvloed. Dit sluit ook in pogings om sodanige aanvalle van 'n opponerende staat en/of entiteit teen te staan. Die kern van hierdie siening is dat inligting as 'n magsinstrument aangewend kan word, in sowel offensiewe as defensiewe rolle. Die definisie vir inligtingsoorlogvoering wat voorgestel word, omvat drie vorme van inligtingsoorlog, naamlik netoorlog, sielkundige operasies en kuberoorlog, wat op 'n kognitiewe/tegnologiese kontinuum gedifferensieer word. Inligtingsoorlogvoering hou veel wyer implikasies vir die gemeenskap in die geheel in, veral in dié genetwerkte tydvak, beide as 'n sekerheidsbedreiging en 'n instrument vir magsprojeksie. Hierdie definisie van inligtingsoorlogvoering bied die geleentheid om die gemeenskaplike grondslae en karaktertrekke van die fenomeen te identifiseer. Hierdie grondslae beklemtoon onder andere die belangrikheid van genetwerkte verhoudings, die inligtingsrevolusie en die digitale eeu wat sentraal ten opsigte van die toekomstige ontwikkeling en manifestasie van die fenomeen is. Terselfdertyd vind moderne oorloë en konflikte ook toenemend binne die konteks van die inligtingseeu plaas, wat die rol van inligtingsoorlogvoering as 'n eietydse nasionale veiligheidsbedreiging vestig. Deeglike ontleding van die manifestasie en implikasies van inligtingsoorlogvoering in die huidige en toekomstige konflikte in Afrika, maar ook wêreldwyd, is 'n noodsaaklikheid om konflik en oorlog in sy moderne en toekomstige konteks te verstaan.

1. Inleiding

Sedert die 1990's is inligtingsoorlogvoering 'n integrale deel van bykans alle internasionale konfliksituasies. Die mees prominente onlangse voorbeelde sluit in die Hamas-Israel-konflik (Desember 2008 tot Januarie 2009), die Georgië-Rusland-oorlog (Augustus 2008) en die Estland–Rusland-kuberoorlog (April 2007).

Ten spyte van die algemene gebruik van die woord *inligtingsoorlogvoering* in sowel die akademie as die media, is dit duidelik dat die inhoud hiervan somtyds verskillend verstaan word. Inligtingsoorlogvoering het 'n gewilde postindustriële oorlogvoering- en magsprojekteringskonsep geword, veral na die einde van die Koue Oorlog. Wat egter in gebreke gebly het, is 'n kritiese beskouing van

ISSN 1995-5928 | Tel: 021 886 5169 | E-pos: akademies@litnet.co.za

bestaande definisies met die doel om dié fenomeen duideliker te verstaan. Beide eng en wye definisies dra daartoe by dat die belangrikheid, en veral moontlike eksponensiale groei, van dié element van oorlogvoering nie na waarde geskat word in óf die akademie óf die wyer media nie.

Inligtingsoorlogvoering word oorspronklik geskep as 'n VSA militêre konsep, ontwerp hoofsaaklik met die doel om voortgesette VSA militêre dominansie in die post-Koue Oorlog-tydvak te verseker. Dit het aanleiding gegee tot 'n uitgebreide korpus werke oor inligtingsoorlogvoering, baie daarvan in die openbare domein (De Landa 1991; Libicki 1995; Schwartau 1996; Waltz 1998 en Denning 1999). Alhoewel die konsep steeds hoofsaaklik in 'n ontwikkelende-wêreld-milieu gebruik en ontwikkel word, begin al hoe meer skrywers van Europa, Australië, China en Indië sedert die laat 1990s ook op die fenomeen van inligtingsoorlogvoering fokus (Hauschild 1999; Ji 1999).

Weens die oorsprong van die konsep is dit nie verbasend dat inligtingsoorlogvoering-verwante taal, metafore en beelde steeds 'n militêre karakter het nie. Dit is so ten spyte daarvan dat baie van die onderliggende beginsels en aannames betekenisvolle nasionaleveiligheidsimplikasies het wat veel wyer strek as bloot die konvensionele militêre invloed (Cronin en Crawford 1999:257). In die konteks van die verruiming van wat as nasionaleveiligheidsbedreigings beskou word, veral as gevolg van globalisasie en die inligtingsrevolusie, is hierdie eng militêre beskouing nie meer houbaar nie. Terselfdertyd word die tradisionele begrip van die militêre domein en oorlogvoering ook toenemend bevraagteken as gevolg van internasionale integrasie en tegnologiese ontwikkeling (Darnton 2006:141). Soos inligting al hoe meer 'n integrale deel van produksie, bestuurstrategieë en modusse van magsprojeksie word, word dit 'n kritieke onderdeel van die 21ste-eeuse opvatting van mag (Kilibarda 2003:10).

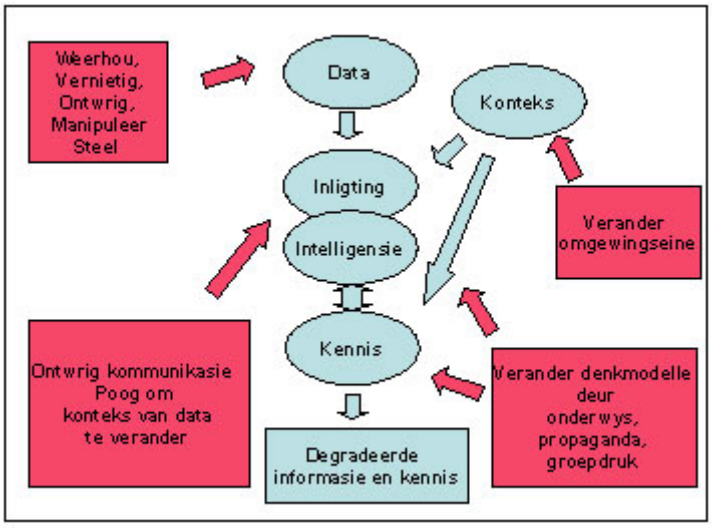
2. Definisie van konsepte relevant tot inligtingsoorlogvoering

Data, inligting, kennis en oorlogvoering is die basiese konsepte wat eers gedefinieer moet word voordat 'n definisie vir inligtingsoorlogvoering bespreek kan word.

As vertrekpunt word die verskille tussen data, inligting en kennis ondersoek. *Data*, *inligting* en *kennis* is in 'n mate meerduidige terme wat tot gevolg het dat daar nie altyd duidelike grense tussen hulle aangedui kan word nie. Ten spyte van dié probleem bestaan daar tog 'n geïmpliseerde hiërargie tussen die konsepte met data as die mees basiese eenheid, kennis op 'n hoër vlak as inligting, en om dit selfs verder te neem, wysheid wat dui op 'n hoë vlak van geleerdheid met genoegsame ondervinding en die vermoë om albei oordeelkundig toe te pas (Webster 2005:187).

Die konvensionele manier om *data*, *inligting* en *kennis* te definieer is liniêr. Sien Illustrasie 1.1 ter illustrasie van hierdie konsepte en moontlike uitdagings.

ISSN 1995-5928 | Tel: 021 886 5169 | E-pos: akademies@litnet.co.za



Illustrasie 1.1 Kontinuum van data, kennis, inligting en intelligensie (Bron: Gebaseer op Hutchinson en Warren 2001: 2)

Data beskryf eienskappe van dinge (Hutchinson en Warren 2001:1), insluitend individuele waarnemings, metings en basiese boodskappe. Databronne sluit in menslike kommunikasie, teksboodskappe, elektroniese navrae en die resultate van wetenskaplike instrumente wat metings neem (Waltz 1998:1–2).

Inligting is georganiseerde en ingesorteerde datastelle in konteks (Hutchinson en Warren 2001:1). Dit is 'n hulpbron bestaande uit twee elemente: fenomene (data) wat waargeneem word, saam met die instruksies (stelsels) wat nodig is om die data te ontleed ten einde dit betekenis te gee (Wilson 2007:2). Die organiseringproses mag insluit sortering, klassifisering, of indeksering en die onderliggende skakeling van data met die doel om die verbande in konteks te plaas vir latere soektogte en ontleding (Waltz 1998:1-2).

'n Verwante maar breër definisie van *inligting*, naamlik "inhoud of betekenis van 'n boodskap" (Mader 1974:3) word in hierdie artikel gebruik. Inligting bly 'n sentrale hulpbron vir kompetisie, konflik en oorlog in state en dit bly van kritieke belang dat hierdie hulpbron akkuraat gedefinieer, gemeet en beoordeel moet word (Waltz 1998:49).

Nadat inligting ontleed en geïnterpreteer word in die lig van ondervinding en begrip, word dit kennis (Hutchinson en Warren 2001:1). Kennis sluit beide die statiese inhoud en die dinamiese prosesse in. In die nasionale-veiligheid-konteks word na hierdie mate van begrip verwys as *intelligensie* (Waltz 1998:1-2). Intelligensie is verwerkte inligting en kennis waarvolgens 'n staat spesifieke voorkomende aksies kan neem. Dit stel sodanige regering in staat om met redelike akkuraatheid te bepaal wat in die toekoms mag gebeur (Johnson 2004).

Verduideliking van hierdie konsepte wat onderliggend aan inligtingsoorlogvoering is, begin reeds dui op die kwesbaarhede wat die vernietiging en/of manipulasie van inligting vir magsprojeksie inhou. Hierdie aksies teen data, inligting, kennis en intelligensie sluit in 'n verskeidenheid direkte en indirekte aksies wat kan lei tot die degradering van inligting en inligtingstelsels.

ISSN 1995-5928 | Tel: 021 886 5169 | E-pos: akademies@litnet.co.za

Oorlogvoering is ’n reeks dodelike en niedodelike aktiwiteite wat onderneem word om die wil van ’n teenstander of vyand te onderdruk. In hierdie sin is oorlogvoering nie sinoniem met oorlog nie. Oorlogvoering vereis nie ’n oorlogsverklaring of ’n toestand alom bekend as ‘n “staat van oorlog” nie. Oorlogvoering kan onderneem word deur, of teen, staatsbeheerde, staatsondersteunde of niestaatsgroepe. Dit is die vyandige aktiwiteit gerig teen ’n teenstander of vyand (Szafranski 1995). In die konteks van inligtingsoorlogvoering is dié direkte dodelike gevolge van oorlogvoering uitgesluit.

Tydens oorlogvoering beskou die partye in die konflik mekaar se doelwitte as wedersyds uitsluitend en pas hulle druk en ander metodes toe om oorwinning te behaal. Inligtingsoorlogvoering plaas die kollig veral op operasies wat die genoemde “ander metodes” gebruik (Waltz 1998:1). Terwyl hierdie standpunt bydra tot die afbakening van inligtingsoorlogvoering, sluit dit steeds ’n beduidende reeks aksies in, wat die identifikasie van inligtingsoorlogvoering verwante aksies problematies maak.

Terwyl inligtingsoorlogvoering ’n spesifieke betekenis in die konteks van hierdie studie het (wat hier onder gedefinieer word), is inligting reeds sedert die begin van die geskiedenis deel van oorlogvoering. Dit is dus ook belangrik om in die definiëring van die konsep duidelik ’n verband, maar ook verskille, te toon tussen nuwe, inligtingseeu- en historiese manifestasies van elemente van inligtingsoorlogvoering.

3. Soeke na ‘n definisie van *inligtingsoorlogvoering*

3.1 Uitdagings in die soektog na ‘n definisie

Alhoewel inligtingsoorlogvoering ’n onlangse konsep is, word ’n wye verskeidenheid betekenisse, sowel as verwante konsepte, soos inligtingsoorlog, kuberoorlogvoering, netoorlog, inligtingsoperasies, bevel-en-beheer-oorlogvoering, kuberaktivisme, netwerkgesentreerde oorlogvoering, operasionele-netwerk-waardering, kuberterrorisme, kubervandalisme en kennisoorlog daaraan geheg. Die verskillende, en somtyds oorvleuelende, aard van al hierdie konsepte het ook bygedra tot die verwarring oor die werklike omvang van die inligtingsoorlogvoeringsfenomeen. In hierdie artikel word die konsep *inligtingsoorlogvoering* gebruik vir ’n oorkoepelende beskrywing van verskillende maar verwante manifestasies en gebruike van inligting in ’n magsprojekteringskonteks. (In die VSA word in plaas van *inligtingsoorlogvoering* 'n term verkies wat as *inligtingsoperasies* vertaal kan word.) Sekere konsepte of dele van konsepte sal egter uitgesluit word in ’n poging om op die betekenis van *inligtingsoorlogvoering* te fokus.

Daar is nie ‘n enkele algemeen aanvaarbare definisie van *inligtingsoorlogvoering* nie (Candolin 2003). Dit is so omdat inligtingsoorlogvoering ’n vinnig-ontwikkelende en tot nou toe onnoukeurig-gedefinieerde onderwerp verteenwoordig wat van groter wordende belang vir vakkundiges, beplanners en beleidsmakers betrokke by nasionale veiligheidsake is. Die belangrikste bronne van beide die belangstelling in en die gebrek aan konsensus oor hierdie terrein is die inligtingsrevolusie gelei deur die vinnige ontwikkeling van die kuberruimte,[1] mikrorekenaars en meegaande inligtingtegnologieë (Molander, Riddile en Wilson 1996:xi).

Een van die doelwitte van oorlogvoering was nog altyd om die inligtingstelsels van die opponent te vernietig, te ontwrig of te beïnvloed. In die breedste konteks

ISSN 1995-5928 | Tel: 021 886 5169 | E-pos: akademies@litnet.co.za

omsluit inligtingstelsels alle metodes waardeur 'n teenstander sekere kennis en opvattings bekom. Volgens 'n enger beskouing word geglo dat inligtingstelsels die middel is waarmee 'n teenstander beheer oor magsprojeksies uitoefen en dit rig.

Saamgevat is inligtingstelsels 'n omvattende stel kennis, denkraamwerke en besluitnemingsprosesse van die teenstander. Die uitkoms wat deur inligtingsaanvalle op alle vlakke bereik wil word, is vir die teenstander om die boodskap te ontvang wat hom sal oortuig dat hy weerstand moet staak (Szafranski 1995).

Die algemene begrip van die belangrikheid van inligtingsoorlogvoering het verander en dit word nie meer net as 'n primêr militêre instrument beskou nie. Inligtingsoorlogvoering hou veel wyer implikasies vir die gemeenskap in die geheel in, veral in die genetwerkte tydvak beide as 'n veiligheidsbedreiging en as 'n instrument vir magsprojeksie. Inligtingsoorlogvoering het ook 'n gewilde konsep in die korporatiewe/ekonomiese, gemeenskaps-/sosiale en persoonlike sfere geword. Sekere inligtingsoorlogvoering-konsepte, -strategieë en -aanwendings is gemeenskaplik tot al hierdie siviele omgewings én die militêre omgewing. Daar is wel vertolkingsverskille, sowel as verskille in die waarneembare wettigheid, etiek en sosiale wenslikheid van die uitkomste wat onder verskillende omstandighede deur die onderskeie spelers nagejaag word (Cronin en Crawford 1999:258).

'n Verdere probleem met die definiëring is verwant aan die omvang van inligtingsoorlogvoering. Verwys *inligtingsoorlogvoering* na die taktiese of die strategiese domein (Taipale 2006, skyfie 30)?

Bestaande definisies van *inligtingsoorlogvoering* het tekortkominge. Die omvattende aard van sommige definisies, sowel as die vaagheid van definisies, is van die vernaamste probleme. Ongelukkig het *inligtingsoorlogvoering* so 'n omvattende term geword dat dit amper 'n toutologie is wat byna alle vorme van konflik insluit (Dinardo en Hughes 1995:4). Die oorheersing van VSA militêrgesentreerde definisies in die bestaande literatuur is ook 'n hindernis in pogings om 'n geskikte definisie te vind.

3.2 Breë definisies

'n Breë definisie wat fokus op die sentrale rol van inligting as deel van die proses om 'n strategiese posisie in te neem word deur Stein (1995:32) voorsien, naamlik: "[I]nformation warfare, in its largest sense, is simply the use of information to achieve our national objectives." Indien dié definisie gebruik word, sal geen diplomatieke, militêre of internasionale interaksie uitgesluit word van die begrip *inligtingsoorlogvoering* nie. Selfs roetine-aksies en -optrede in ooreenstemming met historiese praktyk sou volgens hierdie definisie as deel van inligtingsoorlogvoering beskou kon word.

Denning (1999:12) se poging om die definisie van *inligtingsoorlogvoering* te verdiep deur dit te beskryf as "information in any form and transmitted over any media, from people and their physical environments to print to telephones to radio and television to computers and computer networks", identifiseer die moderne tegnologiese omgewing waarbinne inligtingsoorlogvoering kan floreer. Hierdie definisie onderskei egter nie tussen wat beskou kan word as 'n normale boodskap wat bloot oor dié instrumente gekommunikeer word en dit wat as inligtingsoorlogvoering geïnterpreteer kan word nie.

Libicki (1995:1) is meer spesifiek oor wat as inligtingsoorlogvoering beskou kan word. Hy sluit egter uiteenlopende taktiese en strategiese elemente onder die

ISSN 1995-5928 | Tel: 021 886 5169 | E-pos: akademies@litnet.co.za

konsep in wat enige konstruktiewe poging om die gemeenskaplike elemente van inligtingsoorlogvoering te identifiseer, prakties onmoontlik maak. Volgens hom omsluit inligtingsoorlogvoering sewe verskillende soorte oorlogvoering:

> 1. Bevel-en-beheer-oorlogvoering, wat die doelwit het om die vyand se bevelstruktuur se vermoë om bevele te kommunikeer, te verhoed of te belemmer.
>
> 2. Intelligensiegebaseerde oorlogvoering, wat plaasvind wanneer intelligensie direk in militêre operasies ingevoer word (veral teikeninligting en gevegskadebepalings) eerder as wat dit ingevoer word vir oorhoofse beheer en bevel.
>
> 3. Elektroniese oorlogvoering – die gebruik van operasionele tegnieke, naamlik radio- en elektroniese uitsendings en kriptografie, om die fisiese oordrag van inligting te belemmer.
>
> 4. Sielkundige operasies, wat inligting teen die menslike brein gebruik.
>
> 5. Krakeroorlog – sagtewaregebaseerde aanvalle op inligtingstelsels en wat rekenaarverwante ontwrigting van inligtingstegnologienetwerke en -toepassings tot gevolg het.
>
> 6. Ekonomiese-inligtingsoorlogvoering, wat 'n inligtingsblokkade en inligtingsoorheersing probeer bewerkstellig.
>
> 7. Kuberoorlogvoering – konflik in die virtuele wêreld van die kuberruimte.

Alhoewel byvoorbeeld bevel–en-beheer-oorlogvoering, intelligensiegebaseerde oorlogvoering, elektroniese oorlogvoering en ekonomiese-inligtingsoorlogvoering sekere aksies insluit wat deel uitmaak van inligtingsoorlogvoering, sluit dit ook spesifieke militêre en strategiese fenomene in wat veel breër is as bloot inligtingsverwante aktiwiteite. Mededingende intelligensie kan byvoorbeeld, indien dit binne die etiese reëls bedryf word, nie as inligtingsoorlogvoering beskou word nie. Mededingende intelligensie kan beskou word as 'n besigheidsverwante aktiwiteit, gemik op beter besigheidsbesluitneming ten opsigte van die mededingende omgewing (Society for Competitive Intelligence Professionals 2009).

Nog 'n breë definisie wat spesifiek geformuleer is om ook 'n niemilitêre perspektief te verteenwoordig, word voorgestel deur Jones, Kovacich en Luzwick (2002:5), naamlik dat inligtingsoorlogvoering

> is a coherent and synchronized blending of physical and virtual actions to have countries, organizations, and individuals perform, or not perform, actions so that your goals and objectives are attained and maintained, while simultaneously preventing competitors from doing the same to you.

Hierdie definisie sluit potensieel die meeste aksies in wat deur hierdie akteurs uitgevoer word, en dus ook aksies wat ten doel het om wedersyds voordelige uitkomste te bewerkstellig – nouliks iets wat as inligtingsoorlogvoering beskou kan word.

Curran, Concannon en McKeever (2008:6) beskryf inligtingsoorlogvoering as gemeenskapsvlak-konflik wat deels deur die wêreldwye interverweefdheid van inligting en kommunikasie gevoer word. Hierdie definisie bied 'n bruikbare insig in die breër siening van inligtingsoorlogvoering, maar bied nie 'n verwysing na die

ISSN 1995-5928 | Tel: 021 886 5169 | E-pos: akademies@litnet.co.za

doel van die konflik nie. Dit sou dus moeilik wees om aangeleenthede soos besigheidskompetisie en kriminele aktiwiteite wat nie direk relevant is vir nasionale veiligheid nie, uit te sluit.

3.3 Definisies beperk tot die ITK-komponent

Sommige definisies van inligtingsoorlogvoering is beperk, of grootliks beperk, tot die terrein van aanslae op die inligtingstegnologie-en-kommunikasie- (ITK-) infrastruktuur en -vermoëns van state en/of entiteite. Volgens Elbirt (2003:2-3) kan inligtingsoorlogvoering gedefinieer word as 'n ongemagtigde en doelbewuste aanval op 'n opponent se inligtingsinfrastruktuur deur gebruik te maak van rekenaarindringingstegnieke terwyl die opponent terselfdertyd verhinder word (of dit ten minste so moeilik as moontlik vir hom gemaak word) om soortgelyke aanvalle op die inisieerder se inligtingsinfrastruktuur te doen. Hierdie aanvalle sluit inligtingsmisbruik, weerhouding van diens, en die modifikasie, manipulasie, korrupsie of vernietiging van data in. Hierdie definisie benadruk slegs die tegnologiese aspekte van inligtingsoorlogvoering, en sluit die potensiële strategiese implikasie van sodanige aksies met die meer omvangryke doelwit om die besluitnemingsvermoë, en dus mag, van 'n opponent te ondermyn, uit. Die ITK-verwante konseptualisering van inligtingsoorlogvoering sal vir die doel van die artikel beskou word as kuberoorlog.

3.4 Militêre definisies

Volgens Kuehl (2007:10) word inligtingsoperasies (die voorkeurterm vir inligtingsoorlogvoering in die VSA-weermag) in die Oktober 2003-gepubliseerde *Information Operations Road Map* gedefinieer as die geïntegreerde ontplooiing van die kernvermoëns van elektroniese oorlogvoering, rekenaarnetwerkoperasies, militêre misleiding en operasionele sekerheid in samewerking met spesifieke ondersteunende en verwante vermoëns, met die doel om vyandelike menslike en geoutomatiseerde besluitneming te beïnvloed, ontwrig of korrupteer en terselfdertyd jou eie besluitnemingsvermoë te beskerm. Alhoewel dié definisie ietwat meer gefokus is as dié van Libicki, bly sodanige definisie steeds primêr 'n militêre definisie en sluit 'n reeks aksies in wat buite die veld van inligtingsverwante aktiwiteite lê.

Alger (1996:12) beskryf inligtingsoorlogvoering as

> actions taken to achieve information superiority by affecting adversary information, information based processes, and information systems, while defending one's own information, information based processes and information systems".

Hierdie definisie beskryf die strategiese doelwit van die inligtingsoorlogvoering op 'n duidelike en samevattende wyse. Die definisie se beperking is egter dat dit nie die genoemde aksies duidelik omskryf nie. Selfs met die beperkinge wat die politieke en militêre leiers in die verlede in die gesig gestaar het, was inligtingsoorheersing uiters belangrik vir suksesse in strategiese posisionering tydens oorlogvoering. Wat dus benodig word, is om verder te bepaal wat hierdie aksies behels.

In dié verband voeg Widnall en Fogelman (1997) 'n aksie-element by deur inligtingsoorlogvoering te definieer as

> any action to deny, exploit, corrupt or destroy the enemy's information and its functions; protecting ourselves against those actions and exploiting our own military information functions.

ISSN 1995-5928 | Tel: 021 886 5169 | E-pos: akademies@litnet.co.za

Hutchinson en Warren (2001:2–4) lewer ook 'n bydrae deur inligtingsoorlogvoering te konseptualiseer as 'n aanval op die elemente data, konteks, inligting en kennis (sien Figuur 2.1). Inligtingsoorlogvoering word deur hulle verduidelik as inligtingsoperasies wat gedurende die tyd van krisis of konflik gedoen word met die doel om spesifieke doelwitte ten koste van teenstanders te behaal. Dit is aksies gemik op die beïnvloeding van siviele of militêre besluitneming, operasionele vermoë en die publieke mening deur gebruik te maak van inligting en inligtingsprosessering beide as teiken en as wapen, asook om jouself teen sodanige beïnvloeding te beskerm. Dus het inligtingsoorlogvoering beide 'n offensiewe en 'n defensiewe dimensie. Inligtingsoorlogvoering kan uitgevoer word deur siviele, politieke, sielkundige, sosiale, ekonomiese en militêre metodes op strategiese, operasionele, of taktiese vlakke (Candolin 2003).

Inligtingsoorlogvoering is dus 'n poging om alle fasette van magsprojeksie saam te voeg, gerig teen 'n teenstander op 'n sinergistiese wyse om doelwitte te bereik (Armistead 2004:18). Die meeste van die militêr-georiënteerde definisies verwys na die niemilitêre omgewings waarin inligtingsoorlogvoering kan manifesteer.

3.5 Verband tussen inligtingsoorlogvoering en mag

'n Belangrike aspek wat in baie inligtingsoorlogvoering definisies nie aangespreek word nie, is die verband tussen inligtingsoorlogvoering en mag. Verskeie praktiese en teoretiese aktiwiteite gerig op die manipulasie van data, inligting en kennis dra nie direk by tot die vermindering van 'n regering of regerende elites se politieke, sosio-ekonomiese en militêre mag nie. Sodanige aktiwiteite, wat ekonomiese, sosiale en kriminele doelwitte het, kan nie as inligtingsoorlogvoering in 'n nasionaleveiligheidskonteks gereken word nie.

Nasionale mag is toenemend afhanklik van wye deelname en kompetisie in die skepping en gebruik van dominante tegnologieë (Gompert 1999:59). Die vooruitgang in veral die telekommunikasie-, informasietegnologie- en mediavelde het die magsparadigma oor die afgelope twee dekades verander. Die belangrikheid van inligting as 'n element van mag is in die gebruik van inligting en verbruikbaarheid, wat dit anders maak as in die verlede. Die vermoë om inligting te transformeer, om dit te verskuif, of vir dit om sy mag te vertoon, verwys alles na inligting se oordraagbaarheid. Dit is hiermee dat tegnologie die magstruktuur revolusionêr verander het. Die samevoeging van wat eers afsonderlik gefunksioneer het, het deelname vir almal moontlik gemaak deur toegang tot mag deur die gebruik van inligting en het ook aan mense die geleentheid voorsien om dit wêreldwyd te versprei (Armistead 2004:13).

Inligting het gevolglik enersyds ontwikkel as volwaardige element van nasionale mag saam met diplomatieke militêre en ekonomiese mag, maar andersyds het inligting terselfdertyd interverweef geraak met genoemde ander magselemente (Murphy 2006:vii). Die verbintenis van inligtingsoorlogvoering met die vermoë van die staat om sy magsprojektering in stand te hou en te vergroot, is een van die faktore wat 'n onderskeid maak tussen inligtingsoorlogvoering as 'n nasionaleveiligheidsvraagstuk en inligtingsoorlogvoering as 'n sosiale fenomeen.

3.6 Definisie van *inligtingsoorlogvoering*

Gebaseer op die bostaande evaluasie van verskillende definisies van *inligtingsoorlogvoering* word die volgende definisie vir die konsep voorgestel:

ISSN 1995-5928 | Tel: 021 886 5169 | E-pos: akademies@litnet.co.za

> Inligtingsoorlogvoering is aksies gefokus op die destabilisering of manipulasie van sentrale inligtingsnetwerke van 'n staat of entiteit in 'n gemeenskap met die doel om die vermoë en wil om mag te projekteer, te beïnvloed, asook die pogings om sodanige aanvalle van 'n opponerende staat en/of entiteit teen te staan.

Die fokus van inligtingsoorlogvoering is dus op die ontwrigting en manipulasie van 'n opponent se besluitnemingsprosesse (Wilson 2007:2). Dit kan op twee vlakke plaasvind, naamlik die kognitiewe en tegnologiese vlakke. Voortspruitend hieruit manifesteer inligtingsoorlogvoering op twee verskillende maar tog ook verwante maniere (sien Tabel 1.1). Een manifestasie, wat beide netoorlog en sielkundige operasies insluit, is verwant tot die staat se vermoë en kwesbaarheid ten opsigte van netwerke, persepsies, misleiding, besluitneming, beïnvloeding en kennis. Die tweede, kuberoorlog, verwys na die tegniese infrastruktuur wat die staat se magsvermoë ten opsigte van digitale netwerke, kritieke informasietegnologie-infrastruktuur, sagteware en hardeware aantas. Daar is wel ooreenkomste tussen die twee manifestasies van inligtingsoorlogvoering, maar die belangrikste verskille kom voor op die kognitiewe–tegnologie-kontinuum binne die breër konsep van inligtingsoorlogvoering (sien Illustrasie 1.2).

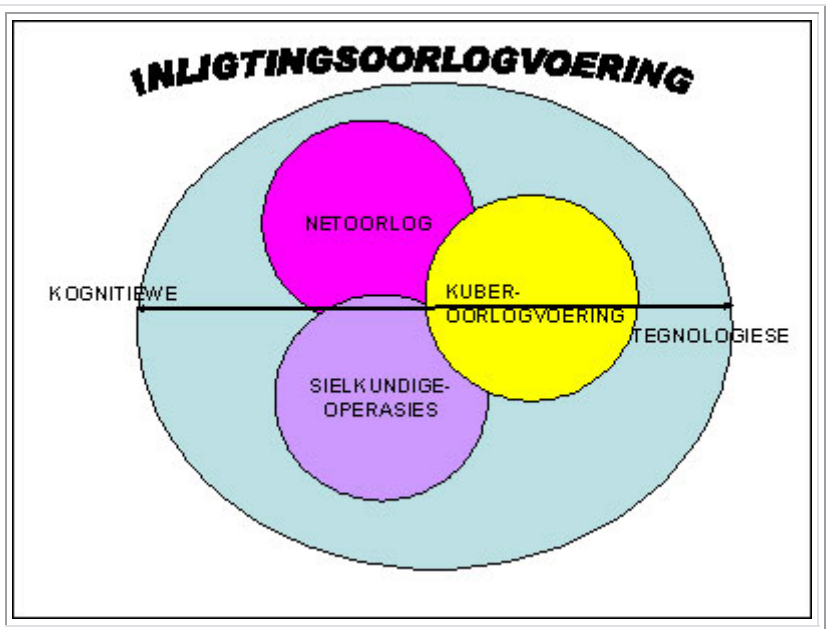
Tabel 1.1 Manifestasie van inligtingsoorlogvoering

Veranderlikes	**Tipe 1: Netoorlog / Sielkundige operasies**	**Tipe 2: Kuberoorlog**
Nasionaleveiligheids-bedreiging	Ja	Ja
Sfeer	Genetwerkte verhoudings / kognitiewe vlak Menslikebesluitnemingsvlak	Kuberruimte- / tegnologiese vlak
Teiken	Genetwerkte verhoudings, besluitnemingsprosesse, persepsies beïnvloed	Inligtingstelsels deur die verandering van data en inligting
Doelwit	Ontwrig besluitneming / Fokus diverse magte op geselekteerde teikens	Ontwrig/korrupteer infrastruktuur van moderne bestuursprosesse
Metode	Invloed binne genetwerkte gemeenskappe en propaganda	Kubermetodes
Benadering	Misleiding	Ontwrigting/ vernietiging
Strategie	Ongelykmatige / gelykmatige strategie	Kuberruimte-operasies
Middele	Massamedia / genetwerkte verhoudings	Internet-/ITK-netwerke
Teenwig	Sosiale netwerke; teenpropaganda en openbare verhoudinge	Netwerksekuriteit

ISSN 1995-5928 | Tel: 021 886 5169 | E-pos: akademies@litnet.co.za

Tegnologie aangewend	Uitsaaiwese / ITK / sosiale netwerke	ITK
Tydlyn	Geskiedenis/Huidige/ Toekoms	Huidige (vroeë stadium) / Toekoms
Omvang	Grootliks strategies, maar ook takties	Grootliks takties (met strategiese implikasies)
Geografiese dimensie	Plaaslik – Globaal	Globaal
Akteurs	Staat en niestaat	Individueel, niestaat en staat
Primêre drywers	Menslike verstand	Tegnologie
Opleidingsgebied	Hoër onderwys / ondervinding	Tegniese opleiding en onderwys / tegniese ondervinding
Gevegsruimte	Verstandruimte	Kuberruimte

Bron: Eie samestelling



1.2: 1.2: Komponente van inligtingsoorlogvoering (Bron: Eie samestelling)

3.7 *Netoorlog*, *sielkundige operasies* en *kuberoorlog* gedefinieer

Netoorlog word soos volg deur Arquilla en Rondfeldt (1997) beskryf:

> Netwar refers to an emerging mode of conflict at societal levels, involving measures short of traditional war, in which the protagonists use network forms of organization and related doctrines, strategies, and technologies

ISSN 1995-5928 | Tel: 021 886 5169 | E-pos: akademies@litnet.co.za

> attuned to the information age. These protagonists are likely to consist of dispersed small groups who communicate, coordinate, and conduct their campaigns in an internetted manner, without a precise central command.

Die omvang van netoorlog lyk ook op die eerste oogopslag wyd te wees, maar daar is 'n onderliggende patroon wat gemeenskaplik is ten opsigte van die manifestasie van netoorlog. Dit is die gebruik van genetwerkte organisasie, strategieë en tegnologieë ingestel op die inligtingseeu (Arquilla, Ronfeldt en Zanini 1999:83).

Nou verbind met die netwerkmodel van netoorlog is die konsep van sielkundige operasies. Dit verwys na 'n nietasbare sfeer in essensie, die konflikarea in die mens se verstand. Die kriteria vir wen en verloor is grootliks kultuurgebonde en bied 'n geleentheid vir manipulasie (Eriksson 1999:58). Strategiese voordeel is nie noodwendig geleë in 'n fokus op feite en getalle nie, maar in "the complementarily and singularity of the brains who interpret them". Nasionale sinmakende vermoë is van groter belang as die elektroniese inligtingshoofweg, volgens Baumard (1996). Die beïnvloeding van die sinmaking behels meer as slegs die gebruik van elektroniese en digitale metodes, in terme van beide netoorlog en sielkundige operasies. Beide van die manifestasies is so oud soos oorlog en konflik, en verskeie historiese voorbeelde bestaan. Die vooruitgang op die tegnologiese terrein, veral ten opsigte van ITK, het 'n impak op effektiwiteit en invloed van beide netoorlog en sielkundige operasies in die 21ste eeu versterk.

Kuberoorlog is 'n term wat gebruik word om die konflik wat in die kuberruimte (die virtuele wêreld en die internet) plaasvind, in plaas van die fisiese wêreld, te omskryf. Dit kan insluit:

- Aanvalle op regerings- en/of militêr-beheerde webtuistes deur toegang te bekom tot vertroulike of geklassifiseerde inligting, deur ontwrigting van funksies, en/of deur agterdeure te skep vir toekomstige ontwrigting.
- Aanvalle op webtuistes met die doel om die webtuistes ontoeganklik te maak.
- Aanvalle op die hoof-diensbedrywe soos krag-, water- en kommunikasiestelsels, wat ontwrigting of totale onderbreking van dienste tot gevolg het.
- Aanvalle op finansiële instellings soos banke en aandelebeurse, wat ontwrigting, onderbreking en/of vals informasie tot gevolg het.
- Aanvalle op sentrale ruggraatinfrastruktuur, bedieners, of ander dele van die internet wat ontwrigting van internetverkeer meebring (Computerhope.com 2007).

Terwyl inligtingsoorlogvoering nog in sy aanvangstadium is, skep dit moontlikhede, tegnieke en instrumente wat toekomstige teenstanders in 'n groter mate teen mekaar se nasionale strategiese bates gaan aanwend. Hierdie bates sluit in die nasionale politieke wil, besluitnemingsprosesse, vermoë om te kommunikeer en die funksionering van die nasionale-infrastruktuur-sektore. Die risiko verbonde aan inligtingsoorlogvoering is nie fisiese vernietiging nie, maar potensieel grootskaalse ontwrigting (Molander, Wilson, Mussington en Mesic 1998:3). Aangesien die moderne beskawing toenemend afhanklik word van genetwerkte ITK-tegnologieë, kan verwag word dat die nasionaleveiligheids-kwesbaarhede van die moderne staat aansienlik gaan toeneem. Hoewel inligtingsoorlogvoering as drie verskillende maar ook verwante manifestasies gedefinieer kan word, is dit moontlik om 'n gemeenskaplike grondslag wat alle vorme van inligtingsoorlogvoering onderlê, te identifiseer.

ISSN 1995-5928 | Tel: 021 886 5169 | E-pos: akademies@litnet.co.za

4. Grondslag van inligtingsoorlogvoering

Deur kennis te neem van die definisie van *inligtingsoorlogvoering* as 'n oorhoofse term, asook die kritiek op bestaande definisies, word die volgende gemeenskaplike grondslae en karaktertrekke van dié fenomeen geïdentifiseer:

- Die bewerkstelliging van inligtingsuperioriteit, veral in die konteks van genetwerkte inligting, is sentraal tot die konsep van inligtingsoorlogvoering.
- Inligtingsoorlogvoering is ten nouste verbind met die gebruik van inligting as 'n instrument vir manipulasie, magsprojeksie, hefvermoë, en die skep van 'n voordeel.
- Eksponensiële groei van tegnologie, globalisasie en die groeiende belangrikheid van genetwerktheid verhoog die toekomstige belangrikheid van inligtingsoorlogvoering.
- *Inligtingsoorlogvoering* verwys na die kognitiewe en tegnologiese ontwrigting verbind met oorlog en konflik, maar nie na die direkte kinetiese aspekte wat met oorlog en terroristiese aktiwiteite geassosieer word nie.
- Die inligtingsrevolusie verleen momentum aan die versterking van netwerke, terwyl die invloed van hiërargiese vorme van mag taan (Arquilla en Ronfeldt 2001:1).
- Die globale netwerk-ekologie is besig om te transformeer van 'n suiwer kommunikasiemedium na 'n sosiale omgewing van groeiende politieke en veiligheidsbelang (Vlahos 1998:77).
- Inligtingsoorlogvoering is in essensie 'n transdissiplinêre konsep wat belange insluit vanuit die politieke, regerings-, tegnologiese, sielkundige, sosiale, media-, ekonomiese en militêre velde.
- Beide offensiewe en defensiewe rolle word voorsien vir inligtingsoorlogvoering.
- Inligtingsoorlogvoering word nie gebind deur geografiese beperkings nie.
- Die koste verbonde aan inligtingsoorlogvoering is heelwat laer as vir ander vorme van magsprojeksie.
- Dit is wydverspreid en beskikbaar aan enige land en in die meeste gevalle ook aan enige individu of groep wat daaroor wil beskik (McLendon 2008). Enkele tegnologiesevaardigheidshindernisse mag in die geval van kuberoorlog bestaan.
- Die toenemende dubbeldoel-aard van inligtingstegnologie het tot gevolg dat verskeie tegnologieë beide militêre en siviele toepassings het (Schneier 2008).
- Inligtingsoorlogvoering is ongelykmatig van aard. Ongelykmatigheid het betrekking op die kwalitatiewe verskille in die middele, waardes en styl van opponerende magte. Sodra 'n staat of entiteit oor 'n meerderwaardigheid in magsprojeksie beskik, is dit die benadeelde opponente wat hulle wend tot onkonvensionele ongelykmatige metodes om dit teen te staan deur die opponent se sterkpunte te vermy en op sy kwesbaarhede te konsentreer (Bishara 2001).

5. Die makroraamwerk waarbinne inligtingsoorlogvoering manifesteer

Inligtingsoorlogvoering moet egter in die konteks van die makroraamwerk van die veranderende aard van oorlogvoering beskou word. Oorlogvoering en die vorme wat dit potensieel en reëel aanneem, kan gesien word as 'n produk van bepaalde politieke, ekonomiese en sosiale strukture en dinamikas. In die informasie-eeu

ISSN 1995-5928 | Tel: 021 886 5169 | E-pos: akademies@litnet.co.za

het die veranderende makrokonteks (polities, ekonomies en sosiaal) ’n bepaalde invloed op oorlogvoering in die geheel. So verduidelik Toffler en Toffler (1993:3) byvoorbeeld dat "(a) revolutionary new economy is arising based on knowledge, rather than conventional raw materials and physical labor. This remarkable change in the world economy is bringing with it a parallel revolution in the nature of warfare."

Oorlogvoering is die bestuur van geweld, nie slegs die uitvoering daarvan nie. Op enkele uitsonderings na behels oorlogvoering die organisasie en bestuur van ‘n uiteenlopende stel vermoëns om definieerbare en meestal meetbare effekte te behaal. Skares en terroriste, daarenteen, ignoreer die reëls in hul soeke na die onbeheerste uitdrukking van passie om die skepping van ’n spektakel amper as ’n doel op sigself te beskou (Libicki 2007:95). Terwyl sodanige groeperinge selde opweeg teen ’n professionele militêre mag, kan verwag word dat dit in die toekoms mag verander.

Net soos die ontwikkeling van tegnologie sentraal was tot die ontstaan van die drie tydvakke, naamlik die landbou-, industriële en inligtingstydvakke, het dié tydvakke die manifestasie van konflik en oorlog beïnvloed. Elkeen van dié tydvakke word gedefinieer deur die primêre bron van welvaart (Toffler en Toffler 1993:21). Die landbou-, industriële- en inligtingsbasisse van welvaart bepaal ook hoe konflik bestuur word. Dit is so omdat die manier waarop welvaart geskep word, grootliks ook bepaal hoe dit versprei word en hoe ’n gemeenskap gestruktureer word (Hammes 2004:10). Verbind aan eienaarskap van welvaart is gemeenskappe se magstrukture en dus ook potensiële foutlyne vir toekomstige konflikte.

Gedurende die landbou-eeu is oorlog gevoer vir die beheer van plaaslike hulpbronne. Die soldate was óf van plaaslike gemeenskappe direk in beheer van die hulpbronne, óf in die geval van feodalisme, opgekommandeerde huurboere. In teenstelling met stamstelsels het die begin van die beskawing aanleiding gegee tot die ontstaan van ’n professionele klas oorlogvoerders. Hierdie klas oorlogvoerders het kenners geword in die toepassing van geweld om die welvaart wat landbou kan produseer, te beskerm. ’n Ander plig was om die heersende klas te beskerm teen die res van die samelewing (Hammes 2004:10-11). Ten spyte van militêre innovasie soos die gebruik van metaal, mobiliteit en masjiene, was militêre vermoëns grootliks beperk tot dit wat in ’n landbougemeenskap geproduseer en onderhou kon word. Hierdie beperkinge het nie die grootste militêre verowerings in die geskiedenis, soos die Romeinse en Mongoolse ryke, verhoed nie, maar gebrekkige tegnologie en beheer het tog die aanwending van militêremagsprojektering aan bande gelê.

Gedurende die industriële eeu, wat in die middel van die 17de eeu begin het, het industrialisasie aanleiding gegee tot die groei van welvaart, terwyl terselfdertyd die vermoë geskep is om wapens op groot skaal te vervaardig. Die industriële tydvak het aanleiding gegee tot prosesse wat massaproduksie moontlik gemaak het. Hulpbronne en bates word daarna ook deur groter gedeeltes van die algemene bevolking beheer. Dit was ook die gevolg met oorlog. Oorlog het nou die aanval van ’n gemeenskap op ’n ander gemeenskap geïmpliseer, somtyds met die betrokkenheid van miljoene individue, insluitend burgerlikes (Toffler en Toffler 1993:21).

Terselfdertyd was daar ’n toename in die gevorderdheid, vernietigende mag en trefafstand van wapenstelsels, sowel as die professionele bestuur van die logistieke steun van militêre magte. Die hoogtepunt van die industriële eeu was die kernwapenvernietiging van Hirosjima en Nagasaki. Dit het die massa-vernietigingspotensiaal van hierdie eeu onderstreep.

ISSN 1995-5928 | Tel: 021 886 5169 | E-pos: akademies@litnet.co.za

Die inligtingseeu het die effektiwiteit van bestuur verhoog en het ook die gebruik van twee nuwe domeine vir magsprojekteringsaktiwiteite, naamlik die kuberruimte en die buitenste ruim, daar gestel. Hammond (2001) argumenteer dat as gevolg van globalisasie en die beskikbaarstelling van nuwe wapenstelsels, die essensie van oorlog besig is om op 'n revolusionêre wyse te verander. Hierdie verandering is nie net beperk tot die nuwe areas van oorlog, naamlik die kuberruimte en buitenste ruimte, nie, maar ook die manier waarop dit plaasvind, asook die spoed van aksie en wapentuig, het getransformeer. Volgens Hammond (2001:3), "we are in the process of transforming space, time, energy, matter and information of war and warfare".

Siviele teikens is ook toenemend besig om die fokus van oorlogvoering te word. Dit sal waarskynlik ook meer opvallend tydens toekomstige konflikte wees waar inligtingsoorlogvoering na verwagting meer prominent sal wees. Terwyl die kern van oorlogvoering nie verander nie, is die karakter van oorlog wel besig om te verander (Tuck 2008:116).

Terwyl insigte oor die implikasie van die inligtingseeu waardevol is om die veranderende aard van oorlog te verstaan, bly dit misleidend om slegs 'n enkele fokus, of slegs een militêre doktrine, as die resep vir toekomstige sukses te aanvaar. Militêre effektiwiteit mag meer te wyte wees aan nietasbare faktore (soos die vermoë om aan te pas relatief tot jou opponent) as aan tegnologiese tasbaarhede soos inligtingstelsels of presisie teikeningsvermoë. Militêre effektiwiteit, in terme van die vermoë om die vyand se konvensionele vermoë te verslaan, kan nie liniêr gelykgestel word met uiteindelike politieke sukses, wat in wese die finale doel van enige konflik behoort te wees, nie (Tuck 2008:118-9).

Die idee van 'n revolusie in militêre aangeleenthede (RMA) is reeds sedert die vroeë 1990's populêr veral binne VSA strategiese geledere. Die RMA, word beweer, is die resultaat van interaksie tussen tegnologiese verandering, stelselontwikkeling, operasionele innovasie en organisatoriese aanpassing. Hierdie ontwikkelinge word saamgevoeg om die karakter en uitvoering van oorlog fundamenteel uit te daag (Larsdotter 2005:135).

RMA is 'n wyer konsep as inligtingsoorlogvoering, maar tog verwant daaraan. Volgens die paradigma van RMA, veral as gevolg van die impak van die inligtingsrevolusie, soos die deursigtigheid van gebeure en die globale onmiddellikheid van verslaggewing, verhoog die belang van konsepte soos inligtingsoorlogvoering. Vir sommiges is "the most - perhaps only – effective weapon in this battlespace (…) information" (Kuehl 2004:4). Een van die veranderings ten opsigte van oorlogvoering en konflik is ook die vervaging van die grense tussen die militêre en burgerlike terreine (Cavelty en Brunner 2007:7), veral ten opsigte van die infosfeer.

Indien die aard van oorlog in die afgelope vyftig jaar in ag geneem word, sal toekomstige oorloë hoofsaaklik sogenaamde lae-intensiteit-konflikte wees. Die term *lae-intensiteit-konflik* is egter misleidend, aangesien sodanige konflikte grootskaalse lewensverlies en infrastruktuurskade tot gevolg kan hê. Die Sri Lanka-offensief gedurende 2009 teen die Tamil Tiere kan as voorbeeld dien. Beide die organisatoriese en toerusting-behoeftes van weermagte wêreldwyd is besig om te verander (van Creveld 1999:33). Sedert 1945 was 90 persent van militêre konflikte burgeroorloë waartydens relatief ongesofistikeerde wapens gebruik is (Tuck 2008:116). Die netwerk- en sielkundige-operasie-element van inligtingsoorlogvoering sal egter toenemend 'n prominente deel van toekomstige konflik vorm.

ISSN 1995-5928 | Tel: 021 886 5169 | E-pos: akademies@litnet.co.za

6. Gevolgtrekking

Terwyl sommige dimensies van inligtingsoorlogvoering so oud soos die mensdom en konflik self is, het die inligtingseeu unieke en nuwe geleenthede geskep vir dit om te manifesteer as 'n opkomende nasionaleveiligheidsbedreiging in die 21ste eeu. Ten spyte van diverse en somtyds teenstrydige definisies wat aan die konsep verleen is, het die inligtingsrevolusie en groeiende globale integrasie verseker dat dit een van die mees betekenisvolle nasionaleveiligheidsbedreigings van ons tyd sowel as die toekoms word. Inligtingsoorlogvoering word gedefinieer as aksies gefokus op die destabilisering of manipulasie van sentrale inligtingsnetwerke van 'n staat of entiteit in 'n gemeenskap met die doel om die vermoë en wil om mag te projekteer, asook die pogings om sodanige aanvalle van 'n opponerende staat en/of entiteit teen te staan. Die kern van hierdie siening is dat inligting as 'n magsinstrument aangewend kan word, beide in offensiewe en in defensiewe kontekste.

Die konteks van konflik waarbinne inligtingsoorlogvoering manifesteer, is ook besig om te verander. Moderne oorloë vind ook toenemend binne die konteks van die inligtingseeu plaas. Dit is so ten spyte van die steeds hoofsaaklik industriële-eeu- en selfs landbou-eeu-manifestasie van konflik in veral die ontwikkelende wêreld. Dominansie en oorwinning ten opsigte van die inligtingsoorlogvoering-dimensie gaan toenemend bepalend word in die toekoms. Die interafhanklikheid en genetwerkte aard van vandag se samelewing gaan dit moeilik, indien nie onmoontlik nie, maak om dié dimensie van toekomstige konflik te ignoreer.

Met hierdie definisie van inligtingsoorlogvoering word gepoog om die kognitiewe en tegniese aspekte van inligtingsoorlogvoering enersyds te onderskei, maar om ook, andersyds, die verband tussen die uitvoering van sielkundige operasies, kuberoorlog en netoorlog te stel. Uiteraard is deeglike analise van die manifestasie van inligtingsoorlogvoering in die huidige konflikte in Afrika, maar ook wêreldwyd, 'n noodsaaklikheid om konflik en oorlog in sy moderne en toekomstige konteks te verstaan. Enige besluitnemer verantwoordelik vir nasionaleveiligheidsbeleid sowel as die uitvoering van strategiese en taktiese aksies om nasionale veiligheid te verseker, gaan toenemend in die toekoms deur hierdie opkomende bedreiging gekonfronteer word.

Bibliografie

Alger, J.I. 1996. Introduction. In Schwartau 1996.

Armistead, L. (red.). 2004. *Information Operations: Warfare and the Hard Reality of Soft Power*. Washington DC: Brassey's.

—. 2007. *Information Warfare: Separating Hype from Reality*. Washington DC: Potomac Books.

Arquilla, J. en D. Ronfeldt. 2001. The Advent of Netwar (Revisited). In Arquilla en Ronfeldt 2001.

—. 1997. Information, Power and Grand Strategy. In Arquilla en Ronfeldt (reds.) 1997.

Arquilla J. en D. Ronfeldt, D. (reds.). 1997. *Athena's Camp: Preparing for Conflict in the Information Age.* Santa Monica: RAND Corporation. MR-880.

ISSN 1995-5928 | Tel: 021 886 5169 | E-pos: akademies@litnet.co.za

Arquilla, J., D. Ronfeldt en M. Zanini. 1999. Networks, Netwar, and Information-Age Terrorism. In Khalilzad en White (reds.) 1999.

Baumard, P. 1996. From InfoWar to Knowledge Warfare: Preparing for the Paradigm Shift. Universiteit van Paderborn. http://gcc.uni-paderborn.de/www/WI/WI2.htm (6 April 2005 geraadpleeg).

Bennett, T., L. Grossberg en M. Morris (reds.). 2005. *New Keywords: A Revised Vocabulary of Culture and Society*. Malden: Blackwell Publishing.
Bishara, M. 2001. An enemy with no forwarding address. *Le Monde Diplomatique*, 3 Oktober. http://mondediplo.com/2001/10/03asymmetry (12 Januarie 2004 geraadpleeg).

Campen, A.D. en D.H. Dearth (reds.). 1998. *Cyberwar 2.0: Myths, Mysteries and Reality*. Fairfax: AFCEA International Press.

Campen A.D. 2008. Cyberwar, Anyone? *SIGNAL Magazine*, Januarie 2008. http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp (3 Januarie 2008 geraadpleeg).

Candolin, C. 2003. A study of infrastructure warfare in relation to information warfare, net warfare, and network-centric warfare. Artikel bekom van die skrywer op 7 Januarie 2004. Voordrag gelewer tydens die 4th Australian Information Warfare & IT Security Conference, Adelaide, Australië, November 2003.

Cavelty, M.D. en E.M. Brunner. 2007. Introduction: Information, Power, and Security: an Outline of Debates and Implications. In Cavelty, Mauer en Krishna-Hensel 2007.

Cavelty, M.D., V. Mauer en S.F. Krishna-Hensel. 2007. *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*. Aldershot: Ashgate Publishing Company.

Computerhope.com, 2007. Cyberwar. *Computerhope.com.* http://www.computerhope.com/jargon/c/cyberwar.htm (11 Desember 2007 geraadpleeg).

Cronin, B. en H. Crawford. 1999. Information Warfare: Its Application in Military and Civilian Contexts. *The Information Society,* 15(4) :257-63.

Curran, K., K. Concannon en S. McKeever. 2008. In Janczewski en Colarik (reds.) 2008.

Darnton, G. 2006. Information Warfare and the Laws of War. In Halpin, Trevorrow en Webb (reds.) 2006.

De Landa, M. 1991. *War in the Age of Intelligent Machines*. New York: Swerve Press.

Denning, D.E. 1999. *Information Warfare and Security*. Reading MA: Addison-Wesley.

Dinardo, R.L. en D.J. Hughes. 1995. Some Cautionary Thoughts on Information Warfare. *Airpower Journal*, Winter 1995:1-10.

Duyvesteyn, I. en J. Angstrom (reds.). 2005. *Rethinking the Nature of War.* Londen: Frank Cass.

ISSN 1995-5928 | Tel: 021 886 5169 | E-pos: akademies@litnet.co.za

Elbirt, A.J. 2003. Information Warfare: Are You At Risk? *IEEE Technology and Society Magazine*, 22(4):13-9.

Eriksson, E.A. 1999. Viewpoint: Information Warfare: Hype Or Reality? *The Nonproliferation Review,* 6(3):57-64.

Gompert, D.C. 1999. Right Makes Might. Freedom and Power in the Information Age. In Khalilzad en White (reds.) 1999.

Halpin, E., P. Trevorrow en D. Webb (reds.). 2006. *Cyberwar, Netwar and the Revolution in Military Affairs.* New York: Palgrave Macmillan.

Hammes, T.X. 2004. *The Sling and the Stone: On War in the 21st Century*. St Paul: Zenith Press.

Hammond, G.T. 2001. Globalization, Technology and the Transformation of the Security Environment: The Real Revolution in Military Affairs. Voordrag tydens 'n byeenkoms van die American Political Science Association in San Francisco, Augustus 2001.

Hauschild, E. 1999. Modern and Information Warfare, a Conceptual Approach, *Studies in Contemporary History and Security Policy*. Vol. 3. Bern: PeterLang.

Hutchinson , W. en M. Warren. 2001. Principles of Information Warfare. *Journal of Information Warfare*, 1(1):1-10.

Janczewski, L. en A.M. Colarik (reds.). 2008. *Cyber Warfare and Cyber Terrorism*. New York: Hershey.

Ji, Y. 1999. The Revolution in Military Affairs and the Evolution of China's Strategic Thinking. *Contemporary Southeast Asia*, Nr. 21, Desember 1999.

Johnson, A.R. 2004. The Top 12 Priorities for Competitive Intelligence. *Aurorawdc.com* http://www.aurorawdc.com/arj_cics_priorities.htm (1 Junie 2009 geraadpleeg).

Jones, A., G. Kovacich en P. Luzwick. 2002. *Global Information Warfare: How Businesses, Governments, and Others Achieve and Attain Competitive Advantages.* Boca Raton: Auerback Publications.

Jordan, D., J.D. Kiras, D.J. Lonsdale, I. Speller, C. Tuck en C.D. Walton. 2008. *Understanding Modern Warfare*. Cambridge: Cambridge University Press.

Kilibarda, K. 2003. Defining Information Warfare. *Infowar Monitor*. 2 Junie. http://www.infowar-monitor.net/modules.php (30 Junie 2004 geraadpleeg).

Khalilzad, Z.M. en J.P. White (reds.). 1999. *The Changing Role of Information in Warfare*. Washington D.C: RAND Project Air Force.

Kuehl, D. 2004. Foreword. In Armistead (red.) 2004.

—. 2007. Information Operations: the Policy and Organizational Evaluation. In Armistead (red.) 2007.

Larsdotter, K. 2005. New Wars, Old Warfare? Comparing US tactics in Vietnam and Afghanistan. In Duyvesteyn en Angstrom (reds.) 2005.

ISSN 1995-5928 | Tel: 021 886 5169 | E-pos: akademies@litnet.co.za

Libicki, M.C. 2007. *Conquest in Cyberspace: National Security and Information Warfare.* Cambridge: Cambridge University Press.

—. 1995. *What is information warfare?* Strategic Forum. Washington, DC: National Defense University, Institute for National Strategic Studies.

Mader, C. 1974. *Information Systems: Technology, Economics, Applications*. Chicago: Science Research Associates, Inc.

McLendon, J.W. 2008. Information Warfare: Impacts and Concerns. *War and Game Webjoernaal*. 24 Februarie.

http://warandgame.wordpress.com/2008/02/24/information-warfare-impacts-and-concerns/ (2 Maart 2008 geraadpleeg).

Molander, R.C., A.S. Riddile en P.A. Wilson. 1996. *Strategic Information Warfare: A New Face of War,* Santa Monica: National Defense Research Institute.

Molander, R.C., P.A. Wilson, D.A. Mussington en R.F. Mesic. 1998. *Strategic Information Warfare Rising.* Santa Monica: Rand Corp.

Murphy, D. 2006. Preface. In Murphy, Groh, Smith en Ayers (reds.) 2006.

Murphy, D., J.L. Groh, D.J. Smith en C.E. Ayers (reds.). 2006. *Information as Power: An Anthology of Selected United States Army War College Student Papers.* Vol. 1. Carlisle: US War College.

Patman, R.G. (red.). 1999. *Security in A Post-Cold War World*. Basingstoke: Macmillan Press.

Schneier, B. 2008. America's Dilemma: Close Security Holes, or Exploit Them Ourselves. *Wired.* 1 Mei. http://www.wired.com/politics/security/commentary/securitymatters/2008/05/blog_securitymatters_0501 (4 Mei 2008 geraadpleeg).

Schwartau, W. (red.) 1996. *Information Warfare. Cyberterrorism: Protecting your Personal Security in the Electronic Age*. 2de uitgawe. New York: Thunder's Mouth Press.

Society for Competitive Intelligence Professionals. 2009. Frequently Asked Questions. *scip.com* http://www.scip.org/resources/content.cfmitemnumber601&nav (1 Junie 2009 geraadpleeg).

Stein, G.J. 1995. Information Warfare. *Airpower Journal*, 9(1):30-39.

Szafranski, R.A. 1995. Theory of Information Warfare: Preparing For 2020. *iwar.org* Gepubliseer in *Airpower Journal.* Lente. http://www.iwar.org.uk/iwar/resources/airchronicles/szfran.htm (10 Januarie 2008 geraadpleeg).

Taipale, K.A. 2006. Deconstructing Information Warfare. Voordrag deur die direkteur van die Center for Advanced Studies in Science and Technology Policy aan die Committee on Policy Consequences and Legal/Ethical Implications of Offensive Information Warfare, Washington D.C. 30 Oktober.

ISSN 1995-5928 | Tel: 021 886 5169 | E-pos: akademies@litnet.co.za

Toffler, A. en H. Toffler. 1993. *War and anti-war: Survival at the dawn of the 21st century*. New York: Little, Brown.

Tuck, C. 2008. Land Warfare. In Jordan, Kiras, Lonsdale, Speller, Tuck en Walton 2008.

Van Creveld, M. 1999. The Future of War. In Patman (red.) 1999.

Vlahos, M. 1998. The emergence of the Infosphere and its Impact on Military Operations. In Campen en Dearth (reds.) 1998.

Waltz, E. 1998. *Information Warfare: Principles and Operations.* Boston: Artech House.

Webster, F. 2005. Information. In Bennett, Grossberg en Morris (reds.) 2005.

Widnall S.E. en R.R. Fogelman. 1997. *Cornerstones of Information Warfare.* Doctrine/Policy Document, United States Air Force.

Wilson, C. 2007. *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues.* CRS verslag vir die Kongres. 20 Maart. Washington DC: Congressional Research Service (CRS).

Eindnotas

[1] Arquila en Ronfeldt (1997:41) beskryf die kuberruimte as 'n bio-elektroniese omgewing wat letterlik universeel is, aangesien dit bestaan oral waar daar telefoonlyne, koaksiale kabels, optiese lyne of elektromagnetiese golwe bestaan. Hierdie omgewing bestaan uit kennis in elektroniese vorm. Die kuberruimte bestaan uit twee meetbare elemente: verbinding en inhoud. Verbinding sluit in die fisiese hardeware, sagteware en kabel- of elektromagnetiese infrastruktuur wat die skepping, oordrag, stoor en deel van data moontlik maak. Die tweede element van die kuberruimte is inhoud wat optrede en besluitneming beïnvloed (Campen 2008).

ISSN 1995-5928 | Tel: 021 886 5169 | E-pos: akademies@litnet.co.za